Hex Five – MultiZone™ Security

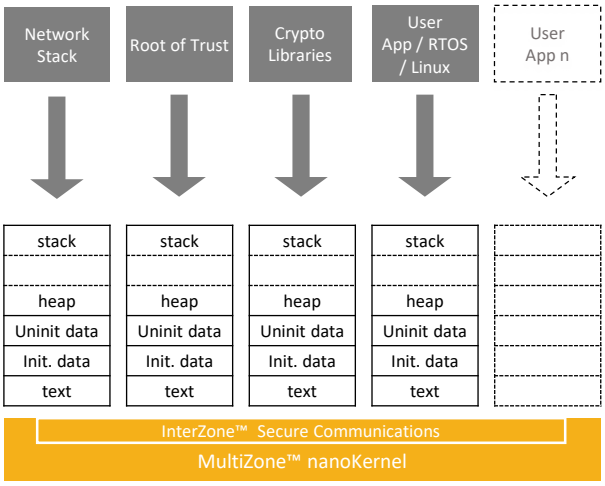
Hex Five Security, Inc. is the creator of MultiZone™ Security, the first Trusted Execution Environment (TEE) for RISC-V. Hex Five's patent pending technology provides policy-based hardware-enforced separation for an unlimited number of security domains, with full control over data, code and peripherals.

What is MultiZone™ Security?

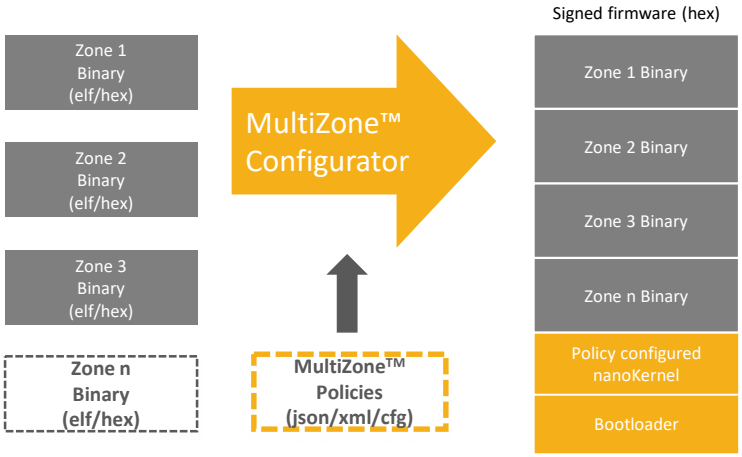
MultiZone™ Security is the first Trusted Execution Environment for RISC-V – it enables development of a simple, policy-based security environment for RISC-V that supports rich operating systems through to bare metal code.

MultiZone™ Security consists of the following components:

- ***MultiZone™ nanoKernel*** – lightweight, formally verifiable, bare metal kernel providing policy-driven hardware-enforced separation of ram, rom, i/o and interrupts.
- ***InterZone™ Messenger*** – communications infrastructure to exchange secure messages across zones on a no- shared memory basis.
- **MultiZone™ Configurator** – combines fully linked zone executables with policies and kernel to generate the signed firmware image.
- **MultiZone™ Signed Boot** – 2-stage signed boot loader to verify integrity and authenticity of the firmware image (sha-256 / ECC)



How does MultiZone™ Security Integrate with Existing Development Environment?



MultiZone™ Security integrates seamlessly into your existing IDE such as Eclipse or command line based toolset.

Application blocks are written, compiled and linked separately for each zone producing a set of elf or hex file.

MultiZone™ Policies are set to achieve the desired ram, rom, i/o and interrupt isolation for each zone – RWX, with granularity down to 4 bytes.

Finally the MultiZone™ configurator is invoked to combine zone elf/hex files with the nanoKernel and bootloader into a signed firmware image.

The full system can be written, compiled and debugged with your existing GNU or Eclipse toolset.

www.hex-five.com

info@hex-five.com

Hex Five – MultiZone™ Security

Hex Five Security, Inc. is the creator of MultiZone™ Security, the first trusted execution environment (TEE) for RISC-V. Hex Five's patent pending technology provides policy-based hardware-enforced separation for an unlimited number of security domains, with full control over data, code and peripherals.

Features

- Preemptive real time scheduler: round robin / cooperative, configurable time tick, cpu overhead < 1%
- Formally verifiable, completely written in assembly, self-contained - no 3rd party library dependencies
- Unlimited number of isolated Trusted Execution Environments (zones) - hardware-enforced, policy-defined
- Up to 16 memory-mapped resources per zone – i.e. flash, ram, i/o, uart, gpio, timers, etc.
- Any combination of top-of-range and naturally aligned configuration – minimum granularity 4 bytes
- Any combination of read, write, execute policy – resource overlapping allowed although not recommended
- Built-in support for fencing configurable on a per-zone basis – i.e. cache / pipeline / instruction / load /store
- Full support for PLIC and CLIC Interrupts – fully configurable zone / interrupt mapping
- Full support for secure user-mode interrupt handlers – even without 'N' extensions
- Full support for low-latency vectored interrupts, preemptable interrupts, and Wait For Interrupt - suspend mode
- Built in trap & emulate for most protected instructions – i.e. CSR read only
- Secure inter-zone communications infrastructure based on messaging - no shared memory / buffers
- C library wrapper for protected mode execution – via ECALL exception handling mechanism
- Signed boot suitable for 2-stage boot room and/or public key / root of trust / PUF – SHA-256 / ECC
- Command line configurator utility compatible with any operating system capable of running Java 1.8

Development Environments

- Eclipse IDE including MCU and GNU Toolchain plugins and OpenOCD / JTAG / GDB live debugging
- Andes AndeSight™ IDE with ICE or OpenOCD debugger
- SiFive FreedomStudio IDE including MCU and GNU Toolchain plugins and OpenOCD / JTAG / GDB live debugging
- Linux and Windows command line tools (make, gcc, gdb, etc.) – native Linux, Java 1.8 required for Windows
- Built-in board support packages for X300 (Rocket), SiFive HiFive Unleashed, E21, E31, E51; Andes N(X)25 and others

System Requirements

- 32 bit or 64 bit RISC-V ISA with 'S' or 'U' extensions
- Physical Memory Protection compliant with Ver. 1.10
- 4KB FLASH and 1KB RAM

Hex Five Security is a proud member of the RISC-V Foundation

HEX-Five Security

RISC-V

www.hex-five.com

info@hex-five.com